sub Office of the
Legislative
Montana State
University --
Bozeman

Office of the Legislative Auditor

State of Montana

Report to the Legislature

June 1995

EDP Audit Report

STATE DOCUMENTS COLLECTION

DEC 20 1995

MONTANA STATE LIBRARY
1515 E. 6th AVE.
HELENA, MONTANA 59620

Montana State University-Bozeman

This report provides information regarding the general controls over the university's computer center. It contains recommendations to the university for improving controls over the university's electronic data processing environment. These recommendations address improving:

- **Electronic access controls.**
- **Physical security controls and establishing formal contingency procedures.**
- **Overall documentation of controls and policies and procedures.**

PLEASE RETURN

Direct comments/inquiries to:
Office of the Legislative Auditor
Room 135, State Capitol
PO Box 201705
Helena MT 59620-1705

95DP-01

Montana State University -- Bozeman :EDP
3 0864 00095915 8

EDP AUDITS

Electronic Data Processing (EDP) audits conducted by the Office of the Legislative Auditor are designed to assess controls in an EDP environment. EDP controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States General Accounting Office.

Members of the EDP audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business and public administration.

EDP audits are performed as stand-alone audits of EDP controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

MEMBERS OF THE LEGISLATIVE AUDIT COMMITTEE

Senator Greg Jergeson, Vice Chairman	Representative Ernest Bergsagel, Chairman
Senator Sue Bartlett	Representative Beverly Barnhart
Senator Reiny Jabs	Representative A. R. "Toni" Hagener
Senator Tom Keating	Representative Bob Keenan
Senator Ken Miller	Representative Robert Pavlovich
Senator Linda Nelson	Representative Bruce Simon

STATE OF MONTANA

Office of the Legislative Auditor

STATE CAPITOL
PO BOX 201705
HELENA, MONTANA 59620-1705
406/444-3122
FAX 406/444-3036

LEGISLATIVE AUDITOR:
SCOTT A. SEACAT

LEGAL COUNSEL:
JOHN W. NORTHEY

DEPUTY LEGISLATIVE AUDITORS:
MARY BRYSON
Operations and EDP Audit
JAMES GILLETT
Financial-Compliance Audit
JIM PELLEGRINI
Performance Audit

June 1995

The Legislative Audit Committee
of the Montana State Legislature:

This report is our EDP audit of general controls relating to the university's centralized data processing center. We reviewed the general controls over the Office of Systems and Computing Services at Montana State University-Bozeman. This report contains recommendations for improving EDP controls at the center. Our findings address improving electronic access, physical security, and overall documentation. The university's written response to our audit recommendations is included in the back of the audit report.

We thank Montana State University-Bozeman Office of Systems and Computing Services for their cooperation and assistance throughout the audit.

Respectfully submitted,

Scott A. Seacat
Legislative Auditor

Office of the Legislative Auditor

EDP Audit

Montana State University-Bozeman

Members of the audit staff involved in this audit were Ken Erdahl and Maureen Leo.

Table of Contents

List of Figures iii

Appointed and Administrative Officials iv

Report Summary S-1

Chapter I - Introduction and Background

Introduction 1

Background 1

Audit Objectives 3

Audit Scope and Methodology 4

Compliance 5

Summary 5

Chapter II - Electronic Access

Introduction 6

Electronic Access Controls 6
- Technical Support Staff Access Should be Limited 7
- Access to System Account Should be Restricted 9
  - Password not Changed 10
- Access to the Audit Journal Should be Restricted 11
- Access to Critical Application Files Should be Restricted . 12
- Programmer Access to Production Programs Should be Limited 13
- Proxy Access Should be Restricted 15
- Access to the System is not Controlled 17

Summary 18

Chapter III - Physical Security Controls and Other Issues

Introduction 19

Physical Security Controls 19
- MSU-Bozeman Should Improve Its Disaster Recovery Plan 19
- OSCS Should Test Existing Physical Security Controls . . 21
  - Preventive Maintenance 22
  - Testing Environmental Control Equipment 22
  - Off-site Storage Facility 23
- Computer Room Access 24

Documentation 25
- System Development 26
  - Documentation of System Changes 26
- General Documentation 27
  - Operating System Documentation 28
  - Employee Terminations and Access 28

Table of Contents

Summary 29

Agency Response Montana State University - Bozeman 33

List of Figures

Figure 1 OSCS Organization 2

Figure 2 MSU-Bozeman Distributed Network - Locations 3

Appointed and Administrative Officials

Board of Regents of Higher Education

		Term Expires
Marc Racicot, Governor*		
Nancy Keenan, Superintendent of Public Instruction*		
Dr. Jeff D. Baker, Commissioner of Higher Education*		
Jim Kaze, Chairman	Havre	1999
Cordell Johnson, Vice Chairman	Helena	1996
Kermit R. Schwanke	Missoula	1997
Paul Boylan	Bozeman	1998
Patrick P. Davison	Billings	2000
L. Colleen Conroy	Hardin	2001
Jim Brown, Student Regent	Butte	1995

*Ex officio members

Commissioner of Higher Education

Dr. Jeff D. Baker	Commissioner of Higher Education
Richard Crofts	Deputy Commissioner for Academic Affairs
Rod Sundsted	Associate Commissioner for Fiscal Affairs
Laurie O. Neils	Director of Budget and Accounting

Montana State University

Dr. Michael Malone	President
Robert M. Specter	Vice President for Administration and Finance
Dr. Thomas H. Gibson	Treasurer for the Vice President of Administration and Finance
V. James Efta	Acting Director of the Office of Systems and Computing Services

Report Summary

Introduction

We performed an Electronic Data Processing (EDP) audit of Montana State University-Bozeman's Office of Systems and Computing Services facility. We reviewed general controls existing within the data processing environment.

Overall, we found the general controls provide for controlled application processing on the mainframe computer system. We found hardware and system software, organizational and procedural controls to be adequate. However, we noted electronic access weaknesses which could compromise application data integrity. The physical security and system development weaknesses we identified could compromise MSU-Bozeman's ability to provide continuous processing services. In addition, we found several areas where documentation of controls and procedures is lacking, which could affect continuity and consistency of operations.

Electronic Access Controls

Access controls provide electronic safeguards designed to protect computer system resources. Proper access controls prevent and/or detect deliberate or accidental errors caused by improper use or unauthorized manipulation of data, programs, and/or computer resources. System security can limit access to specific areas. Limited access based on job duties prevents users from inadvertently or willfully executing programs or changing data unrelated to their job. System security is especially critical given the fact that the MSU-Bozeman system is accessible, through modem and INTERNET, from nearly anywhere in the world.

Technical Support Staff Access Should be Limited

Access to the VAX/VMS operating system is controlled in part by the allocation or denial of privileges to individual user accounts. During our review we found that some of the critical privileges have been allocated to several OSCS technical support staff who did not need the privileges to perform their jobs. This condition leads to increased possibilities of unauthorized access and/or damage to the system.

Some system activities can only be performed by users who hold specific privileges. These restrictions protect the integrity of the operating system's performance and, thus, the integrity of service

provided to users. Privileges should be granted to user accounts based on two factors: 1) whether the user has a legitimate need for the privilege, and 2) whether the user has the skill and experience to use the privilege without disrupting the system.

When users have critical privileges, the operating system and service to others can be disrupted. Such disruptions can include failure of the system, destruction of data, and exposure of confidential information. Critical privileges granted to users should be reviewed, and restricted to only those individuals who require it in the performance of their jobs.

Access to SYSTEM Account Should be Restricted

We found nine OSCS personnel have access to the SYSTEM account through a shared password. This allows those individuals write access to everything on the system, with no means of determining who made changes while logged in under the account. Access to this account should be restricted to only those persons needing it in the performance of administrative and security functions.

Access to this account by several individuals with a shared password exposes the system to accidental or intentional changes to the system files and programs. For example, since SYSTEM has BYPASS privilege, users could delete any file no matter what its protection. If they type an incorrect name or accidental asterisk, they may destroy files they or other users need to keep. The access needed by various individuals should be re-assessed and appropriate access should be given to those individuals. Access to the SYSTEM account should be limited and logged.

Password not Changed

A logon ID unique to a specific computer user and protected by a password known only to that user provides a good means of limiting access to appropriate users and helps provide accountability for work done. Periodic changing of the passwords reduces the risk the password will be guessed by someone other than the user.

We found MSU-Bozeman does not force changing of the password for the SYSTEM account. The password on this account is changed only as determined necessary, usually between 90 and 180

days. Considering the unlimited access that is available to users through the SYSTEM account, we believe MSU-Bozeman should require forced changing of the password for the account every 90 days or less to reduce the risk of unauthorized persons gaining inappropriate access to the system.

Access to the Audit Journal Should be Restricted

The VMS operating system contains a feature that will log activity for certain files in an "audit journal", for review by the security officer. We found full write access to the audit journal file is available to several people within OSCS. Because of the security related nature of the audit journal, access to view and change entries in the journal should be restricted to the security officer and system administrator. When individuals have access to change this file the logging function becomes an ineffective security tool.

Within the logging function, there are several security reporting functions that can be enabled. We found the following functions were not enabled for the MSU-Bozeman system: INSTALL, which would log all installations of images; LOGIN (DIALUP), which would log all logins via modem; and FILE_ACCESS, which would log all accesses to critical system and/or application files using "all" privileges. We believe MSU-Bozeman should restrict access to the audit journal and enable the security functions, to provide additional protection to the system.

Access to Critical Application Files Should be Restricted

There are several files within any application that are critical to its operation. These include source code, command files, and executable files. We found all of the OSCS operators and some of the system programmers have access to read, write, execute, and delete the files.

These files are critical to the operation of MSU-Bozeman administrative and other applications, and unlimited access by several people exposes them to unauthorized and/or unintentional change or deletion. This puts the applications at risk for potential abuse. Access to these files should be restricted to only those

individuals needing it in the performance of their jobs, and any changes to the files should be logged.

Programmer Access to Production Programs Should be Limited

We determined at least 13 programmers have unrestricted and unlogged access to the SIS, HRS, and FRS application production programs and data. Industry standards suggest management prohibit programmer access to production programs and data. In addition, Montana Operations Manual section 2-1210.00, states no one person should be in a position to perpetrate and conceal errors and irregularities. The present access allows programmers the potential to change student enrollment data, grades, accounts receivable, employee payroll data, and/or accounting transactions without authorization.

We believe programmer access to the production programs and data should be eliminated. MSU-Bozeman should review programmer access and limit it to only those requiring it to correct errors or resolve programming problems. In addition, the system provides a logging function which MSU-Bozeman currently does not use. Using this function, all activity within a specified file or program would be recorded and could be reviewed by the security officer. We believe MSU-Bozeman should enable the logging function for the application production programs and files, and the security officer should review it on a daily basis.

Proxy Access Should be Restricted

The VAX/VMS system at MSU-Bozeman is a distributed system. This means there are several individual networks that can work independently, or interface with the other networks. Individual logins are required for each of the individual networks. For those individuals who use the various networks regularly, this requires a separate ID and password for each network. In order to reduce that inconvenience, the VMS system provides a process called "proxy." A proxy login will cause some or all of the distributed networks to recognize an ID from another network, and when requested, will automatically log that ID on to the receiving network. During the transfer of the proxy information between networks, a sophisticated user may be able to intercept the process and gain access through that account. Any privileges on the

account would be available to the intruder, as if the intruder were the valid user.

During our review we evaluated the use of proxy accounts in the MSU-Bozeman system. We determined MSU-Bozeman has not implemented adequate controls over the use of proxy accounts. This exposes the system to inappropriate use and manipulation by unauthorized users. In order to prevent this exposure, MSU-Bozeman should evaluate its use of proxy access and at a minimum implement controls recommended by the DEC security manual.

Access to the System is not Controlled

During our review, we found several individuals within OSCS with access beyond what is required in the performance of their jobs. When we questioned OSCS personnel as to why they had that level of access, they were unable to explain. Personnel were not certain who authorized the access, or for what reason they were given the access. Since access privileges allow access to critical files and programs on the system, authorization and approval of that access should be controlled.

We believe that whenever a person requests an account with privileges above the minimum, MSU-Bozeman should require a form which documents the reason for the access and evidence of review and approval by a supervisor and security personnel. Many of the access problems we found during our review may have been prevented if the users were required to justify their access needs through the use of access request forms.

Physical Security Controls

Physical security controls can improve the separation of custody over assets, prevent the accidental or intentional destruction of data, and provide for both the replacement of records that may be destroyed and the continuity of operations following a major hardware or software failure. Physical security controls include: safeguarding of files, programs and documentation; physical safeguarding of the computer facility; and a plan or method to ensure continuity of operations following major destruction of files or hardware breakdown.

We reviewed existing physical controls in place at the OSCS facility. We noted computer hardware was installed on a raised floor, smoke alarms function properly, air conditioning maintains controlled computer room temperature, and the power supply meets computing equipment needs. However, we noted instances where OSCS could improve physical controls over computer operations.

MSU-Bozeman Should Improve Its Disaster Recovery Plan

The Office of Systems and Computing Services has a disaster recovery plan which outlines the general procedures to be followed in the event of major hardware or software failure. We reviewed the plan and found it did not outline specific procedures, nor did it identify responsibilities for individuals involved in the recovery. Without a detailed plan, recovery of the system could be delayed unnecessarily.

Documented and tested recovery procedures allow normal operations to resume as quickly as possible following a disaster. Without a formal disaster recovery plan, MSU-Bozeman may be unable to process accounting transactions, pay employees, or process student enrollment records. This could become even more critical if some of the MSU satellite campuses begin sharing the MSU-Bozeman computer system.

OSCS Should Test Existing Physical Security Controls

The MSU-Bozeman computer room is equipped with various environmental control equipment to help protect the computer equipment from damage due to water, temperature, and physical intrusion. Various alarms are in place to alert the employees in the room. In addition, some of the alarms are connected to an independent security systems contractor for 24-hour electronic surveillance. We reviewed OSCS procedures for monitoring and testing the environmental control equipment. We identified the following concerns with OSCS procedures.

Preventative Maintenance

Maintenance of the environmental alarms and equipment is performed by various individuals. In some cases, we could not determine who was responsible for the various maintenance tasks. OSCS personnel were unsure as to who performed the maintenance, if or when it was done, and what specific procedures were followed. We believe OSCS management should schedule, monitor, and log all preventive maintenance to ensure the maintenance is done as scheduled, by whom it is done, and what specific tasks are performed.

Testing Environmental Control Equipment

During our review, we determined that testing of environmental control equipment, and training on the use of the equipment, was lacking. We determined the water detection alarm in the computer room had not been tested for some time. We believe the operators may not be able to determine the source of the alarm, nor would they know the procedures to follow in the event they could determine the source of the alarm. We could not determine if there had been testing of the heat detector. In addition, we determined there had been no formal training on the use of some of the safety equipment in recent years. Therefore, safe and efficient use of the equipment is questionable.

Off-site Storage Facility

We also reviewed physical controls at the off-site storage facility. The storage facility contains the backup tapes from the system, to be used in case the information on the system is lost or destroyed. We found physical controls at the off-site facility to be insufficient. The tape cabinets were susceptible to water damage, temperature and humidity damage, and fire hazards.

The backup tapes are essential to the recovery process in the event data or equipment is damaged or destroyed. With inadequate protection against environmental hazards OSCS management cannot be assured the tapes will be usable when they are needed. Subsequent to our audit and discussions with OSCS management, MSU-Bozeman moved the off-site storage facility to a different location. The new location should provide a more secure environment with improved environmental controls.

Computer Room Access

During our review, we found four groups of people are given access codes and keys to the computer room, for after-hours access. These people include the operations personnel, network services personnel (systems programmers), and hardware maintenance personnel within OSCS. The fourth group consists of the Facilities Services custodians. Industry standards recommend that programmers and custodians not have unrestricted access to computer hardware and files. The computer room is staffed for 17 hours every working day. We believe access should be denied to the programmers and custodians, except while the room is staffed. This would reduce the risk of intentional or accidental damage to the computer hardware.

As an additional service of the security systems contractor, OSCS could have all access to the computer room logged. This would provide a record of when the room was accessed, and to which group the person belongs. We believe the logging service could provide for additional accountability of the people with access to the computer room, and allow management a means for review of computer room access.

Documentation

According to industry standards, "Management should require various levels of documentation and establish formal procedures to define the system at appropriate levels of detail." In addition, state law requires internal evaluations related to specific general controls. In our review of MSU-Bozeman general controls, we found areas where general documentation is lacking or non-existent. We noted the following areas where documentation should be improved.

System Development

The Information Services (IS) function of OSCS provides programming support to administrative system Data Base Managers. Services include programming to modify or enhance existing computer applications. IS guidelines provide for documented programming changes and testing procedures. In addition, IS employees regularly consult with application coordinators to facilitate support request services. We reviewed services IS provides to academic and administrative departments.

We found areas where IS could improve its documentation of internal operations to ensure services meet user needs.

Documentation of System Changes

IS employees submit requests for changes to the existing applications (SIS, HRS and FRS) to the Data Base Manager (DBM). The DBM then must present the request to a Module Team. A Module Team, which consists of users, programmers, and management personnel, reviews the requests for changes and approves and prioritizes them. The team meetings are not documented, and the change requests are not formalized through documentation. Therefore, the changes may not be done according to the original request, and there is no record of what the original intent of the change was. Proper documentation could ensure the requested change is approved, and the ability to determine whether the changes are performed as requested.

We believe review and approval by the Module Team should be documented, and properly completed change request forms should be required for all changes to the applications. This would provide documentation of the supervising analyst's authorization for completed programming changes. Authorized documentation also enables management to address subsequent questions from the application owner.

General Documentation

OSCS has not documented all its policies and procedures associated with the implementation and maintenance of computer general controls. We believe MSU-Bozeman should establish policies which encourage OSCS to adopt procedures which include, but are not limited to, the following:

1. Conduct and periodically update a comprehensive risk analysis to determine security threats to data and information resources.
2. Develop and periodically update written policies and procedures which provide security over data and information resources.
3. Implement appropriate cost-effective safeguards to reduce, eliminate, or recover from identified risks to data and information resources.

4. Perform periodic internal audits and evaluations of the security program for data and information resources.

MSU-Bozeman provided internal policies and procedures for the OSCS function but did not provide overall computing policies and procedures. We discussed documentation in several areas of this report where general documentation could be improved. By not documenting its policies, procedures, and controls, MSU-Bozeman cannot ensure compliance with state law, consistency of operations or continuity of services.

Chapter I - Introduction and Background

Introduction

We performed an Electronic Data Processing (EDP) audit of Montana State University-Bozeman's Office of Systems and Computing Services facility. We reviewed general controls existing within the data processing environment.

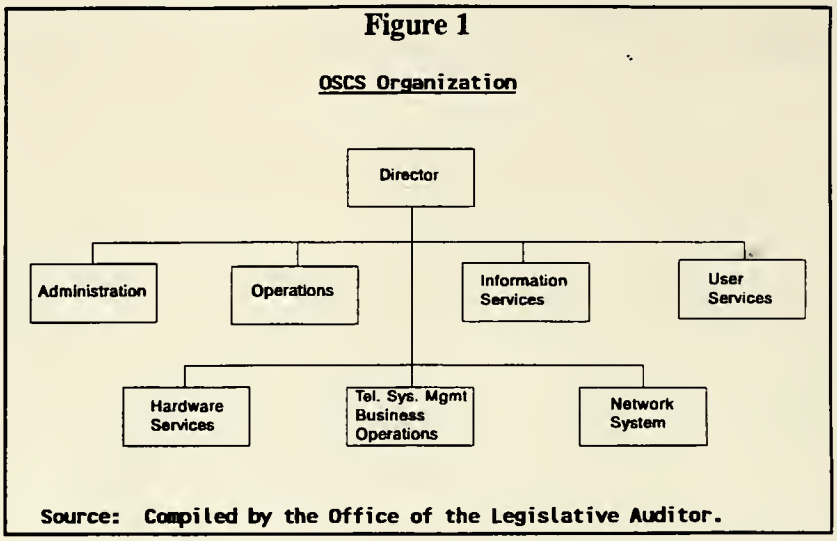
General controls are a component of the overall internal control environment of computer-based applications. Data processing general controls are designed to ensure computer programs work consistently and properly; data files and resources are accessed only as authorized; and the entire data processing operation is adequately protected to ensure continued operation during normal and contingency situations.

Background

Montana State University-Bozeman (MSU-Bozeman) was founded on February 15, 1893. MSU-Bozeman is a land-grant institution as authorized by the Morrill Act of 1862 and receives part of its support from land-grant income as well as from state appropriations, student fees, and federal and private grants. MSU-Bozeman is a part of the Montana University System. In 1994 the Montana Board of Regents restructured the university system. Effective July 1, 1994, Montana State University at Bozeman was combined with several other units of the system: Eastern Montana College, Northern Montana College, the Great Falls Vocational Technical Center and the Billings Vocational Technical Center, to form Montana State University. The EDP audit was limited to the Bozeman campus of Montana State University.

The Office of Systems and Computing Services (OSCS) provides the support necessary to address the computing and information systems requirements of the research, instructional and administrative programs at MSU-Bozeman. OSCS is comprised of seven divisions: Administration, Operations, User Services, Hardware Services, Information Services, Network Systems, and Telecommunications Systems Management and Business Operations (See Figure 1). Responsibilities of OSCS include programming, software and hardware installation and maintenance, and problem resolution for the 10,000 plus users of the MSU-Bozeman computer system.

Figure 1

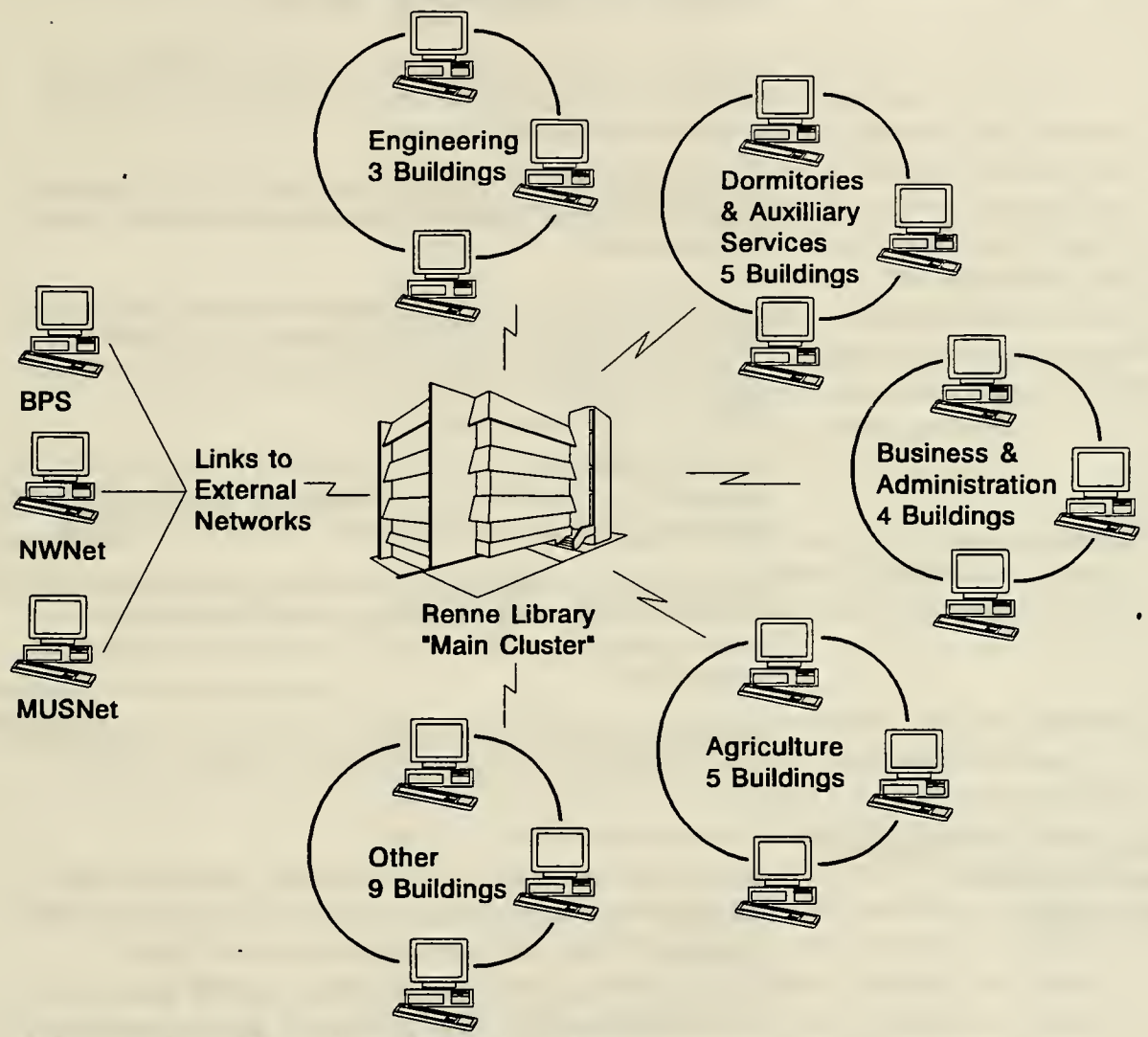


Source: Compiled by the Office of the Legislative Auditor.

OSCS computer operations are based around Digital Equipment Corporation (DEC) computer systems. The MSU-Bozeman computer system is "distributed" in nature. It is comprised of over 1000 network nodes (individual computers) residing in 26 network-connected buildings (See Figure 2). The system consists of several networks which are able to operate independently of each other. All of the networks are connected through a communications link which allows users to transfer information, and facilitates maintenance and backup to remote networks. OSCS manages some of the networks, while others are autonomous but contract with OSCS for particular services, such as backup or INTERNET connectivity. Although the system is distributed, MSU-Bozeman has combined some networks with common features and interfaces into "clusters." The "main cluster," located at the Renne Library, contains the applications for MSU-Bozeman administration.

Figure 2

MSU-Bozeman Distributed Network - Locations



Source: Compiled by the Office of the Legislative Auditor.

Audit Objectives

The objective of this EDP audit was to determine the adequacy of general controls specific to MSU-Bozeman's Office of Systems and Computing Services (OSCS) facility. A general control review includes an examination of the following controls:

Organizational - apply to the structure and management of the computing and information services facility. Specific types of organization controls include segregation of duties, assignment of responsibilities, rotation of duties, and supervision.

Procedural - include operating standards and procedures which ensure the reliability of computer processing results and protect against processing errors.

Hardware and Software - represent controls within the operating system software and hardware which monitor and report system error conditions.

System Development - include oversight and supervisory controls imposed on development projects. Controls include feasibility studies, development, testing and implementation, documentation, and maintenance.

General Documentation - apply to all aspects of the computing and information services facility. Documentation includes policies and procedures which ensure consistent and continuous operations.

Physical Security - are physical site controls which include security over access to the computer facility, protection devices such as smoke alarms and sprinkler systems, and disaster prevention and recovery plans.

Electronic Access - allow or disallow user access to electronically stored information such as data files and application programs.

Audit Scope and Methodology

The audit was conducted in accordance with government audit standards. We compared existing general controls against criteria established by the American Institute of Certified Public Accountants, General Accounting Office, the EDP industry, the DEC and VMS security manuals, Board of Regents policies and the Montana Operations Manual (MOM).

We reviewed MSU-Bozeman's general controls related to the OSCS computer environment. The mainframe computer processes several applications including the Student Information System (SIS), Human Resource Services (HRS), and the Financial Reporting System (FRS). SIS contains student data such as registration information, financial aid information, and transcripts. HRS contains payroll and personnel information, and FRS is the accounting system for MSU-Bozeman. We interviewed OSCS

personnel to gain an understanding of the hardware and software environment at MSU-Bozeman. We also examined documentation to supplement and confirm information obtained through interviews.

We examined procedures within the mainframe environment intended to ensure computer processing activities are controlled. For example, we determined whether mainframe equipment is maintained in a secured area and access is limited to authorized personnel. We also reviewed job control procedures designed to ensure integrity of all system processing. We evaluated the OSCS organizational structure to determine segregation of duties, and system development procedures to ensure applications are designed to process as intended. We did not review controls established by computer users to supplement OSCS general controls.

Compliance

We reviewed compliance with applicable state laws and rules and Board of Regents' policies. We found MSU-Bozeman to be in compliance with applicable laws and Board of Regents' policy.

Summary

We organized the report into three chapters. Chapter I contains the introduction, background information, and audit objectives. Chapter II discusses electronic access and Chapter III provides our findings related to physical security and other general control issues. Overall, we found the general controls provide for controlled application processing on the mainframe computer system. We found hardware and system software, organizational and procedural controls to be adequate. However, we noted electronic access weaknesses which could compromise application data integrity. The physical security and system development weaknesses we identified could compromise MSU-Bozeman's ability to provide continuous processing services. In addition, we found several areas where documentation of controls and procedures is lacking, which could affect continuity and consistency of operations.

Chapter II - Electronic Access

Introduction

MSU-Bozeman's mainframe computer center is located in the basement of the campus library building. Academic and administrative employees and students process programs and data stored on the mainframe through personal computers and terminals located at various campus departments or computer labs. This chapter discusses our review of OSCS procedures intended to ensure electronic access over mainframe operating software, computer programs, and data is controlled.

Electronic Access Controls

Access controls provide electronic safeguards designed to protect computer system resources. Login IDs and passwords control access to MSU-Bozeman's operating system, computer programs, and data. System and application programmers have the highest degree of technical expertise in the computer facility and, therefore, play an important role in maintaining the application. However, application owners have primary responsibility for maintaining adequate controls. Without controls, system and application programmers may conceal changes to programs and data.

Proper access controls prevent and/or detect deliberate or accidental errors caused by improper use or unauthorized manipulation of data, programs, and/or computer resources. System security can limit access to specific areas. Limited access based on job duties prevents users from inadvertently or willfully executing programs or changing data unrelated to their job. System security is especially critical given the fact that the MSU-Bozeman system is accessible, through modem and INTERNET, from nearly anywhere in the world.

MSU-Bozeman uses VAX/VMS operating system software to control electronic access to the operating system, application programs, and data stored on the mainframe computer. The VAX/VMS operating system provides various levels of access. The first level, the login ID, provides system access. The security officer assigns privileges to that ID which allow the holder to access various parts of the system and to perform security tasks. The second level is the assignment of user IDs to one or more groups. The next level is file access. File access can be allowed or restricted through Access Control Lists (ACLs). The ACLs

specify what level of access (read, write, allocate, or delete) an ID or group has to that file. ACL access restrictions can be bypassed if the ID has certain system privileges. In addition, MSU-Bozeman controls access to the SIS, FRS, and HRS applications through application security programs which limit access to programs, data, and specific screens. We reviewed access security established through these security systems and identified areas where OSCS should improve access controls. Our findings are discussed in the following sections.

Technical Support Staff Access Should be Limited

As previously discussed, access to the VAX/VMS operating system is controlled in part by the allocation or denial of privileges to individual user accounts. Privileges range from the basic mailbox privilege, which allows the user to access E-mail, to a group of critical (or "all") privileges. "All" privileges allow the user, through various avenues, to circumvent security and potentially control the system. During our review we found that some of the critical privileges have been allocated to several OSCS technical support staff who did not need the privileges to perform their jobs. This condition leads to increased possibilities of unauthorized access and/or damage to the system.

Some system activities can only be performed by users who hold specific privileges. These restrictions protect the integrity of the operating system's performance and, thus, the integrity of service provided to users. Privileges should be granted to user accounts based on two factors: 1) whether the user has a legitimate need for the privilege, and 2) whether the user has the skill and experience to use the privilege without disrupting the system.

We identified three types of user accounts: 1) an individual account, where the individual is accountable for the use and protection of the account number, 2) a generic interactive account, where several people may have access to the account, and no one person is held accountable for the use of the account, and 3) a generic non-interactive account, which is accessed by a control job, and requires no human interaction.

Of the "all" privileges identified in the VMS Guide to System Security manual, we identified four that are of particular concern:

SETPRV privilege allows the user to enable any or all privileges. The VMS security manual recommends only system managers and security managers have this privilege. On the main cluster alone, we found 17 individual accounts, 9 generic interactive accounts, and 4 generic non-interactive accounts with SETPRV privilege.

SYSPRV privilege allows the user to change a file's protection to gain access to it. The VMS security manual recommends only system managers and security managers have this privilege. On the main cluster we found 17 individual accounts, 8 generic interactive accounts, and 5 non-interactive accounts with SYSPRV privilege.

CMKRNL privilege allows the user to execute a restricted routine. The VMS security manual recommends this privilege be granted only to users who need to execute privileged instructions or who need to gain access to the most protected and sensitive data structures and functions of the operating systems. We identified seven individual accounts, four generic interactive accounts, and two non-interactive accounts with CMKRNL privilege to the main cluster.

BYPASS privilege gives the user access to read, write, execute, and delete any and all files, bypassing all security protection. The VMS security manual recommends this privilege be reserved for use by either well-tested, reliable programs and command procedures or the system backup operation. The manual also recommends this privilege be granted with extreme caution, as it overrides all file protection. We identified four individual accounts, four generic interactive accounts, and one non-interactive account with BYPASS privilege to the main cluster.

When users have these privileges, the operating system and service to others can be disrupted. Such disruptions can include failure of the system, destruction of data, and exposure of confidential information.

OSCS personnel indicated these privileges are necessary to run particular programs and routines. However, for specific routines which require privileges, other access methods are available (such as individual file ACLs). Use of other methods would allow the individual to perform the required task without giving the user global privileges to the entire system.

Recommendation #1

We recommend MSU-Bozeman review the access privileges granted to users and restrict the "all" privileges to only those individuals who require it in the performance of their jobs.

Access to SYSTEM Account Should be Restricted

When a VAX/VMS system is installed, some pre-established accounts are set up for the purpose of allowing the user to have complete access to the system to perform installation and update procedures. These accounts have unlimited privileges to the system, and once the system is installed, they should be deleted or access to them carefully restricted. One of these accounts is the SYSTEM account. We found nine OSCS personnel have access to the SYSTEM account through a shared password. This allows those individuals write access to everything on the system, with no means of determining who made changes while logged in under the account.

The SYSTEM account should be used only for system functions such as performing backups and installing maintenance updates. Access to this account should be restricted to only those persons needing it in the performance of those functions. OSCS personnel indicated systems and operations personnel need access to SYSTEM in order to perform various management functions. However, for day-to-day system management activities, the individual accounts should be given the necessary privileges and access to the SYSTEM account should be suspended.

Access to this account by several individuals with a shared password exposes the system to accidental or intentional changes to the system files and programs. For example, since SYSTEM has BYPASS privilege, users could delete any file no matter what its protection. If they type an incorrect name or accidental asterisk, they may destroy files they or other users need to keep.

Access to the SYSTEM account should be limited. The access needed by individuals to perform various management functions should be re-assessed and appropriate access should be given to those individuals. The operating system provides some options for improving controls over this account. For example, access can be given to specific files or programs, or specific privileges could be given to the individuals, as needed, and then suspended until needed again. In addition, the operating system provides a means for tracking (logging) any event specified by the security officer. Logging and reviewing activity by individuals using the SYSTEM account could help ensure access through this account is appropriate.

Recommendation #2

We recommend MSU-Bozeman:

A. Restrict access to the SYSTEM account to the system administrator and the security officer.

B. Log all access through the SYSTEM account.

Password not Changed

A logon ID unique to a specific computer user and protected by a password known only to that user provides a good means of limiting access to appropriate users and helps provide accountability for work done. Periodic changing of the passwords reduces the risk the password will be guessed by someone other than the user.

We found MSU-Bozeman requires passwords be changed at least every 90 days for most accounts. However, for the SYSTEM account, MSU-Bozeman does not require the password to be changed. The password on this account is changed only as determined necessary, usually between 90 and 180 days. Considering the unlimited access that is available to users through the SYSTEM account, we believe access to the account should be limited to two OSCS personnel (the security officer and system administrator). Also, MSU-Bozeman should require forced

changing of the password for the account every 90 days or less to reduce the risk of unauthorized persons gaining inappropriate access to the system.

Recommendation #3

We recommend MSU-Bozeman require forced changing of the password to the SYSTEM account at regular intervals.

Access to the Audit Journal Should be Restricted

The VMS operating system contains a feature that will log all events specified by the security officer. For instance, if management is concerned about access to critical files by MSU-Bozeman personnel, the logging function will be turned on for that file. Then any activity on that file by any individual will be recorded in the "audit journal" log. The log can then be reviewed by the security officer to determine who made the changes and whether the changes were appropriate.

We found full write access to the audit journal file is available to all OSCS operations personnel, everyone who has access to the SYSTEM account (all Network Systems personnel), and all persons with BYPASS privilege. Because of the security related nature of the audit journal, access to view and change entries in the journal should be restricted to the security officer and system administrator. When individuals have access to change this file the logging function becomes an ineffective security tool.

Within the logging function, there are several security reporting functions that can be enabled. We found the following functions were not enabled for the MSU-Bozeman system: INSTALL, which would log all installations of images; LOGIN (DIALUP), which would log all logins via modem; and FILE_ACCESS, which would log all accesses to critical system and/or application files using "all" privileges (such as BYPASS, SYSPRV and SETPRV).

As noted on pages 7 through 9, BYPASS, SYSPRV, and SETPRV privileges allow a user unrestricted access to all files on the

system. Logging of these privileges would provide a means of monitoring all changes made through them to ensure the changes are appropriate.

OSCS personnel indicated that even if someone has access to the audit journal, they still need to know how to reformat the data into readable format in order to make sense of the information, thus rendering the information useless to most individuals. However, there is considerable technical expertise within OSCS, and we believe they have the knowledge to reformat the report. Also, all OSCS personnel have the ability to delete all or part of the entries directly from the audit journal.

Recommendation #4

We recommend MSU-Bozeman:

A. Restrict access to the audit journal file to the security officer and system administrator.

B. Enable the security alarms INSTALL, LOGIN, and FILE_ACCESS.

Access to Critical Application Files Should be Restricted

There are several files within any application that are critical to its operation. These include source code, which is the programmable code for the various programs; command files, which are the computer operating commands; and executable files, which are the computer readable programs.

Access to source code, command files, and program executable files is controlled by restricting access within the files. The present rights in the MSU-Bozeman system allow all of the OSCS operators and some of the system programmers access to read, write, execute, and delete the files.

These files are critical to the operation of MSU-Bozeman administrative and other applications, and unlimited access exposes

them to unauthorized and/or unintentional change or deletion. This puts the applications at risk for potential abuse. Access to these files should be restricted to only those individuals needing it in the performance of their jobs. As discussed previously, logging access to critical files and applications helps ensure changes made to the files are appropriate and authorized.

Recommendation #5

We recommend MSU-Bozeman:

A. Restrict access to the critical application files to only those individuals needing it in the performance of their jobs.

B. Log and review all access to the critical application files.

Programmer Access to Production Programs Should be Limited

MSU-Bozeman processes several mainframe applications including the Student Information System (SIS), Human Resource System (HRS), and the Financial Reporting System (FRS). These applications process student information, employee payroll records, and budget and accounting data, respectively. MSU-Bozeman assigns a Data Base Manager to administer and manage each application. The managers are responsible for overall application security, data integrity, and enhancements. The Information Services (IS) function of OSCS provides programming services for system users at the request of the Data Base Managers.

During our review, we determined at least 13 programmers have unrestricted and unlogged access to the SIS, HRS, and FRS application production programs and data. Industry standards suggest management prohibit programmer access to production programs and data. In addition, Montana Operations Manual section 2-1210.00, states no one person should be in a position to perpetrate and conceal errors and irregularities. The present access allows programmers the potential to change student enrollment data,

grades, accounts receivable, employee payroll data, and/or accounting transactions without authorization.

IS programmers indicated they require access to correct transaction entry errors or programming code. They noted errors often occur during production data processing and require programmers to resolve the error. We believe MSU-Bozeman could limit programmer access to production programs and data without impacting programmer performance. For example, programmer access to production programs could be enabled temporarily, then disabled once the problem is fixed. For situations where programmer access is required, OSCS could provide a before and after snapshot of programming changes for management's review.

We believe programmer access to the production programs and data should be eliminated. Programming changes and subsequent testing should be done in the test environment. Once the changes are tested and approved, someone other than the programmers could copy the changed programs into production. MSU-Bozeman personnel indicated limited staff and daily programming tasks make total programmer restriction unfeasible. However, MSU-Bozeman should review programmer access and limit it to only those requiring it to correct errors or resolve programming problems. In addition, the system provides a logging function which MSU-Bozeman currently does not use. Using this function, all activity within a specified file or program would be recorded and could be reviewed by the security officer. We believe MSU-Bozeman should enable the logging function for the application production programs and files, and the security officer should review it on a daily basis.

Recommendation #6

We recommend MSU-Bozeman:

A. Limit programmer access to production programs and data.

B. Log and review all programmer activity relating to the production programs and data.

Proxy Access Should be Restricted

As described on page 2 and illustrated in Figure 2, the VAX/VMS system at MSU-Bozeman is a distributed system. This means there are several individual networks that can work independently, or interface with the other networks. Individual logins are required for each of the individual networks. For those individuals who use the various networks regularly, this requires a separate ID and password for each network. In order to reduce that inconvenience, the VMS system provides a process called "proxy." A proxy login will cause some or all of the distributed networks to recognize an ID from another network, and when requested, will automatically log that ID on to the receiving network. During the transfer of the proxy information between networks, a sophisticated user may be able to intercept the process and gain access through that account. Any privileges on the account would be available to the intruder, as if the intruder were the valid user.

Allowing proxy logins effectively merges the security of the affected systems. Therefore, the security is only as good as the security of the least secure system involved. In order to prevent penetration of the system by unauthorized personnel, the DEC security manual recommends the following precautions in relation to proxy access:

1. "Verification" must always be enabled, especially when proxy logins are permitted. This is necessary to prevent someone on another node from intercepting the proxy login and using it to access the system.

2. The parameter INCOMING for proxy should not be used for vital systems. With INCOMING disabled, a proxy login can be used to connect from that system to another, but will not allow incoming proxies to log onto the system.

3. Never set up a proxy account with privileges that could damage the system. Because of the vulnerability of proxy logins, as described above, any proxy logins that are allowed should have very limited access privileges.

During our review we evaluated the use of proxy accounts in the MSU-Bozeman system. We determined MSU-Bozeman has not implemented adequate controls over the use of proxy accounts. As discussed above, enabling "verification" is of particular importance when the proxy logins are privileged accounts, as is the case at MSU-Bozeman. We determined that verification is not enabled on the MSU-Bozeman VMS system.

In addition, as discussed on page 2, the main cluster contains several applications, including the SIS, FRS, and HRS applications. We determined both INCOMING and OUTGOING are enabled on the main cluster. To prevent unauthorized access to the critical information contained on the main cluster, the parameter INCOMING should be disabled. We also found that several of the proxies relating to the main cluster had "all" privileges, which allow the user the ability to control the system. This exposes the system to inappropriate use and manipulation by unauthorized users. In order to prevent this exposure, MSU-Bozeman should evaluate its use of proxy access and at a minimum implement the controls recommended by the DEC security manual.

Recommendation #7

We recommend MSU-Bozeman:

A. Review the "verification" function, and enable it if security will be enhanced.

B. Disable the INCOMING parameter for the main cluster.

C. Review all proxy logins and eliminate unnecessary proxy logins with privileges.

Access to the System is not Controlled

As noted on pages 7 through 9, we found several individuals within OSCS with access beyond what is required in the performance of their jobs. When we questioned OSCS personnel as to why they had that level of access, they were unable to explain. Personnel were not certain who authorized the access, or for what reason they were given the access. Since access privileges allow access to critical files and programs on the system, authorization and approval of that access should be controlled.

We found OSCS uses access request forms only for non-MSU-Bozeman accounts for billing purposes, but does not require access request forms for students or employees. MSU-Bozeman personnel indicated that given the large number of students and employees, an access request form for each person would not be feasible. They also did not believe the forms were necessary since privileges above the basic system required privileges are given only to personnel within OSCS and security personnel know those people personally.

As indicated by MSU-Bozeman personnel, accounts with privileges above the minimum represent a small percentage of total users. We believe that whenever a person requests an account with privileges above the minimum, MSU-Bozeman should require a form which documents the reason for the access and evidence of

review and approval by a supervisor and security personnel. Many of the access problems we noted earlier and discussed on pages 7 through 17 may have been prevented if the users were required to justify their access needs through the use of access request forms. In addition, it would provide a means of review for MSU-Bozeman management.

Recommendation #8

We recommend MSU-Bozeman require authorized access request forms for all individuals requesting privileges above the minimum.

Summary

Tighter security on the MSU-Bozeman system and other systems becomes more and more critical with the continued advancement of technology. MSU-Bozeman is connected to the INTERNET "information highway." Through INTERNET, users from nearly anywhere in the world can gain initial connection to the MSU-Bozeman computer system. This greatly increases the risk that computer users may attempt to gain access to confidential information, and/or make changes to the system. With the access control weaknesses described in this chapter, sophisticated users may be able to penetrate the security of the system and gain access to both system and application files. MSU-Bozeman management and security personnel should consider these risks in their overall computer security plan.

Chapter III - Physical Security Controls and Other Issues

Introduction

This chapter discusses our review of OSCS's procedures which ensure physical security over mainframe hardware and continuity of operations. In addition, we discuss issues relating to documentation.

Physical Security Controls

Physical security controls can improve the separation of custody over assets, prevent the accidental or intentional destruction of data, and provide for both the replacement of records that may be destroyed and the continuity of operations following a major hardware or software failure. Physical security controls include: safeguarding of files, programs and documentation; physical safeguarding of the computer facility; and a plan or method to ensure continuity of operations following major destruction of files or hardware breakdown.

We reviewed existing physical controls in place at the OSCS facility. We noted computer hardware was installed on a raised floor, smoke alarms function properly, air conditioning maintains controlled computer room temperature, and the power supply meets computing equipment needs. However, we noted instances where OSCS could improve physical controls over computer operations. These issues are discussed in the following sections.

MSU-Bozeman Should Improve Its Disaster Recovery Plan

The Office of Systems and Computing Services has a disaster recovery plan which outlines the general procedures to be followed in the event of major hardware or software failure. We reviewed the plan and found it did not outline specific procedures, nor did it identify responsibilities for individuals involved in the recovery. In addition, OSCS does not have an uninterruptable power supply (UPS) installed for its mainframe computing system. During a power failure, a UPS maintains temporary power and allows personnel to complete an orderly shutdown of computer hardware. MSU-Bozeman uses a power conditioner to reduce hardware damage during sudden changes. However, the power conditioner does not prevent hardware shutdown during complete power outages.

Discussions with management indicate they have not identified a need for a detailed recovery plan or a UPS, since the MSU-Bozeman system is distributed, and any one of the distributed networks could be recovered on one of the other networks. However, MSU-Bozeman has not tested recovery on another network using backup tapes. In addition, the information contained on the main cluster far exceeds the capacity of the other remote networks. Therefore, only partial recovery to one of the other networks would be possible if the main cluster was disabled. MSU-Bozeman would need to establish priorities to determine which parts of the system are more critical than others. Without a detailed plan, recovery of the system could be delayed unnecessarily.

Industry standards support management development of formal procedures to efficiently recover computer processing activities to normal operations following a disaster. Section 2-15-114(3), MCA, requires department heads to implement safeguards to reduce, eliminate, or recover from identified threats (which could include power outages) to data and information technology resources. In addition, section 1-0240.00, MOM, outlines agency responsibilities regarding disaster recovery which include assigning recovery team member responsibilities; assessing information and resource requirements necessary to maintain applications; and determining alternate procedures which may be necessary if recovery cannot be completed timely.

A disaster recovery plan may include but is not limited to:

- An inventory of current applications, operating system programs, telecommunications programs or networks, and hardware.
- Identification of the most probable types of risks MSU-Bozeman may face.
- An analysis to determine application significance and impact of loss.
- An analysis to determine application recovery priority.
- Selecting a disaster recovery method depending on how long the organization can operate without processing, management's backup procedures, and cost.

- Identification, involvement, and commitment of employees responsible for operating applications.

- Definition of application requirements including personnel, hardware, system support programs, communications, data, special forms, etc.

Documented and tested recovery procedures allow normal operations to resume as quickly as possible following a disaster. Without a formal disaster recovery plan, MSU-Bozeman may be unable to process accounting transactions, pay employees, or process student enrollment records. This could become even more critical if some of the MSU satellite campuses begin sharing the MSU-Bozeman computer system.

Recommendation #9

We recommend MSU-Bozeman:

A. Establish a detailed disaster recovery plan.

B. Test the plan.

OSCS Should Test Existing Physical Security Controls

The MSU-Bozeman computer room is equipped with various environmental control equipment to help protect the computer equipment from damage due to water, temperature, and physical intrusion. Various alarms are in place to alert the employees in the room. In addition, some of the alarms are connected to an independent security systems contractor for 24-hour electronic surveillance. We reviewed OSCS procedures for monitoring and testing the environmental control equipment. We identified several concerns with OSCS procedures and discuss those in the following sections.

Preventive Maintenance

Maintenance of these environmental alarms and equipment is performed by various individuals. Some maintenance is performed by MSU-Bozeman facilities services, some by the security systems contractor, and some by the OSCS staff. In some cases, we could not determine who was responsible for the various maintenance tasks. OSCS personnel were unsure as to who performed the maintenance, if or when it was done, and what specific procedures were followed. We believe OSCS management should schedule, monitor, and log all preventive maintenance to ensure the maintenance is done as scheduled, by whom it is done, and what specific tasks are performed.

Testing Environmental Control Equipment

Through discussions with various employees of OSCS, we determined many were unsure about how to operate some of the equipment, and what was the appropriate action to take in case one of the alarms goes off. For example, we tested the water detection alarm in the computer room. The alarm is located under the raised floor, and emits an audio alarm as well as an unmarked visual alarm at the operator's console. From our interviews, we determined the alarm had not been tested for some time, and the operators may not be able to determine the source of the alarm, nor would they know the procedures to follow in the event they could determine the source of the alarm.

The heat detector is connected to the contractor's alarm system, and is triggered when the temperature goes above or below certain levels. We were not able to determine when or how that system was last tested.

The computer room is equipped with an automatic halon fire extinguisher system. If the halon alarm goes off, personnel in the computer room have three minutes to determine if there is a fire, and locate it. If it is determined there isn't a fire, the operator can abort the system. If the system is not aborted, the halon will be discharged. We found some operations personnel were unsure where the abort switches were located, or what action to take in the event the alarm was triggered. There are also two hand-held halon fire extinguishers and one CO2 extinguisher. We determined there had been no formal training on the use of the safety equipment in recent years. Therefore, safe and efficient use of the equipment is questionable.

We believe MSU-Bozeman personnel should be trained and knowledgeable about the environmental control systems within the computer room, and be able to operate them efficiently and effectively in the event of an emergency. Insufficient knowledge of the operation of those devices could result in unnecessary loss of equipment, data, or personal injury.

MSU-Bozeman personnel indicated training is provided to the employees on a regular basis, and training manuals also outline the proper use and maintenance of the equipment and procedures. However, there is no documentation of training provided to the users, and our observations indicated the training wasn't provided regularly to all affected employees.

Off-site Storage Facility

We also reviewed physical controls at the off-site storage facility. At the time of our audit the facility was located in the basement of a campus building. The storage facility contains the backup tapes from the system, to be used in case the information on the system is lost or destroyed. We found physical controls at the off-site facility to be insufficient. One of the tape cabinets sits directly on the floor, which makes it susceptible to flood damage. Water pipes are located directly over the cabinets. Temperature and humidity are not controlled. The building is not equipped with a fire suppression system, and there were no fire alarms or fire extinguishers in the room. In addition, the room was cluttered with boxes and papers, which makes it a potential fire hazard.

The backup tapes are essential to the recovery process in the event data or equipment is damaged or destroyed. With inadequate protection against environmental hazards OSCS management cannot be assured the tapes will be usable when they are needed. Subsequent to our audit and discussions with OSCS management, MSU-Bozeman moved the off-site storage facility to a different location. The new location should provide a more secure environment with improved environmental controls.

Recommendation #10

We recommend MSU-Bozeman:

A. Schedule preventive maintenance and testing of existing environmental controls, and maintain documentation of the maintenance and testing completed.

B. Train OSCS employees on the proper use and maintenance of the environmental controls.

C. Ensure its off-site storage facility is located in a secure location where the risk of damage from environmental hazards is minimized.

Computer Room Access

The computer room is staffed from 7:00 a.m. through midnight on every weekday, except holidays. For all other hours, the room is locked, and any access during those hours is monitored through the contractor's alarm system. To gain access to the computer room when it is not staffed, a person needs a key to the door plus a code to disable the alarm.

During our review, we found four groups of people are given access codes and keys to the computer room. These people include the operations personnel, network services personnel (systems programmers), and hardware maintenance personnel within OSCS. The fourth group consists of the Facilities Services custodians. Industry standards recommend that programmers and custodians not have unrestricted access to computer hardware and files. With access to the computer room, the programmers could potentially make and conceal unauthorized changes to the system. OSCS personnel indicated they believe programmer access is necessary for them to perform after-hours maintenance. In addition, they believe after-hour access by the custodians is necessary because the custodians' schedule does not allow them to clean the computer room during regular hours. Given the fact the room is staffed for 17 hours every working day, we believe the access should be denied to the programmers and custodians. They should be required to perform their duties while the room is staffed. This

would reduce the risk of intentional or accidental damage to the computer hardware.

As an additional service of the security systems contractor, OSCS could have all access to the computer room logged. This would provide a record of when the room was accessed, and to which group the person belongs. However, OSCS has opted not to use the logging service. We believe the logging service could provide for additional accountability of the people with access to the computer room, and allow management a means for review of computer room access.

Recommendation #11

We recommend MSU-Bozeman:

A. Restrict computer room access for systems programmers and custodians to hours when the room is staffed.

B. Enable the access logging function offered by the security contractor.

Documentation

According to industry standards, "Management should require various levels of documentation and establish formal procedures to define the system at appropriate levels of detail." In addition, state law requires internal evaluations related to specific general controls. In our review of MSU-Bozeman general controls, we found areas where general documentation is lacking or non-existent. We noted the following areas where documentation should be improved.

System Development

The Information Services (IS) function of OSCS provides programming support to administrative system Data Base Managers. Services include programming to modify or enhance existing computer applications. IS employees provide ongoing programming assistance for SIS, HRS, and FRS applications. Staff programmers are assigned to specific applications and report job progress to senior analysts and the IS manager. IS guidelines provide for documented programming changes and testing procedures. In addition, IS employees regularly consult with application coordinators to facilitate support request services. We reviewed services IS provides to academic and administrative departments. As discussed in the following section, we found areas where IS could improve its documentation of internal operations to ensure services meet user needs.

Documentation of System Changes

IS employees submit requests for changes to the existing applications (SIS, HRS and FRS) to the Data Base Manager (DBM). The DBM then must present the request to a Module Team. A Module Team, which consists of users, programmers, and management personnel, reviews the requests for changes and approves and prioritizes them. The team meetings are not documented, and the change requests are not formalized through documentation. Therefore, the changes may not be done according to the original request, and there is no record of what the original intent of the change was.

Industry standards suggest management establish procedures to ensure system enhancements/modifications are completed according to the application owner's request. Although IS has established policies and procedures for system development services, which require review and approval by the Module Teams, the approval process is not documented. Proper documentation could ensure the requested change is approved, and the ability to determine whether the changes are performed as requested.

Documentation provides a source of information for systems analysts and programmers who are responsible for maintaining and revising existing systems and programs; a basis for training new programming personnel; and a source of information needed to provide continuity in the event of loss of experienced personnel.

We believe review and approval by the Module Team should be documented, and properly completed change request forms should be required for all changes to the applications. This would provide documentation of the supervising analyst's authorization for completed programming changes. Authorized documentation also enables management to address subsequent questions from the application owner.

Recommendation #12

We recommend MSU-Bozeman:

A. Document Module Team review and approval of system changes.

B. Require authorized change request forms for system programming changes.

General Documentation

OSCS has not documented all its policies and procedures associated with the implementation and maintenance of computer general controls. We believe MSU-Bozeman should establish policies which encourage OSCS to adopt procedures which include, but are not limited to, the following:

1. Conduct and periodically update a comprehensive risk analysis to determine security threats to data and information resources.

2. Develop and periodically update written policies and procedures which provide security over data and information resources.

3. Implement appropriate cost-effective safeguards to reduce, eliminate, or recover from identified risks to data and information resources.

4. Perform periodic internal audits and evaluations of the security program for data and information resources.

MSU-Bozeman provided internal policies and procedures for the OSCS function but did not provide overall computing policies and

procedures. We discussed documentation in several areas of this report and found general documentation could be improved by including:

1. Provisions for security against the accidental loss or destruction of records and assurance of continuous operation of its computer system. (See page 19).

2. Procedures for documenting, reviewing, testing, and approving systems, programs, and changes. (See page 26).

3. Controls over access to equipment and data files, including access request forms. (See page 6).

4. Operating system documentation. (See subsequent section).

5. Other procedural controls affecting overall EDP operations. (See subsequent section).

By not documenting its policies, procedures, and controls, MSU-Bozeman cannot ensure compliance with state law, consistency of operations or continuity of services.

Operating System Documentation

OSCS completes periodic installation and upgrades to the VMS operating system. We found that during VMS installation and upgrades, procedures, testing, and problems were not documented. The VMS manual suggests several steps to ensure the software is installed correctly and is secure from outside intrusion. The manual includes a checklist which ensures critical items are not overlooked. We found OSCS maintained no documentation of what was done during installation, what problems were encountered and how they were resolved, and what testing was performed to ensure the system was operating correctly. In addition MSU-Bozeman keeps no record of software upgrades and changes. Lack of documentation on VMS upgrades could result in duplication of effort, inconsistent procedures being followed, not knowing what testing, if any, was done, by whom, and why.

Employee Terminations and Access

MSU-Bozeman has implemented procedures for ensuring terminated employees and students are suspended from the system on a timely basis. While these procedures may be effective in ensuring terminated employee's access is removed from the system, they are not documented to provide information in the event the present personnel are not able to perform that task. In addition,

we found OSCS does not require access requests be documented and authorized. A weakness in or lack of access controls increases the opportunity for unauthorized modifications to files and programs, as well as misuse of the computer hardware. They also decrease the integrity of the system.

Summary

Although OSCS maintains documentation of some policies and procedures, we believe improvements could be made. MSU-Bozeman personnel believe that due to the dynamics of the computer environment, it is impossible to document all aspects of its system. However, if management does not establish formal procedures to create and maintain adequate documentation, there is a risk that applications or systems may not be well documented. Good documentation procedures facilitate system recovery, program modifications, and staff training. At a minimum, a written manual of systems and procedures should be prepared for all critical computer operations and should provide management's general or specific authorization to process transactions. MSU-Bozeman should retain copies of authorizations and their effective dates for systems changes that have been implemented.

Recommendation #13

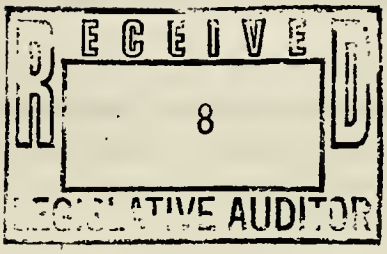
We recommend MSU-Bozeman review present policies and procedures, and ensure critical processes are thoroughly documented, to ensure continuity of operations.

Agency Response

MONTANA STATE UNIVERSITY
BOZEMAN

Office of the President
211 Montana Hall
MSU • Bozeman
Bozeman, MT 59717-0242
Telephone (406) 994-2341
Fax (406) 994-1893

June 6, 1995



Mr. Scott Seacat
Legislative Auditor
P.O. Box 201705
Helena, MT 59620-1705

Re: Campus EDP Audit

Dear Scott:

Attached are the responses of Montana State University - Bozeman for the EDP audit report recently completed by your staff. I am pleased with the outcome of the report, and we very much appreciate the independent and objective evaluation and review conducted on our EDP operations. As we strive to serve the many and diverse needs of our students, faculty, and staff with computing resources which are changing almost on a daily basis, we try to also preserve the integrity of our systems, networks, and data. With the advent and tremendous growth in the use of the Internet, our challenges in maintaining a secure and controlled environment have rapidly mounted.

As you can see from our responses, we are in agreement with the audit recommendations, and have in fact, already taken several steps to implement several of the recommendations. We maintain our commitment to delivering high quality computing services to our faculty and students, and to other users in State government. Without creating undue barriers, we also maintain our commitment to provide controlled access and a secure system to maintain the integrity of the data within. The results of your EDP review have been most helpful to us in identifying those few areas where security can be enhanced to the benefit of all users. I look forward to meeting with you and the members of the Audit Committee and to discussing this.

Sincerely,

Michael P. Malone
President

cc: Commissioner of Higher Education

Recommendation No. 1

We recommend MSU-Bozeman review the access privileges granted to users and restrict the "all" privileges to only those individuals who require it in the performance of their jobs.

Response No. 1

We concur. The Office of Systems and Computing Services (OSCS) has implemented an internal policy and procedure providing a formal method of authorizing privileges beyond minimal (NETMBX and TMPMBX) as well as requiring an annual review of those accounts.

Recommendation No. 2

We recommend MSU-Bozeman:

A. Restrict access to the SYSTEM account to the system administrator and the security officer.

B. Log all access through the SYSTEM account.

Response No. 2

A. We concur.

B. We concur. The SYSTEM accounts will have all access logged.

Recommendation No. 3

We recommend MSU-Bozeman require forced changing of the password to the SYSTEM account at regular intervals.

Response No. 3

We concur. The SYSTEM accounts will have their passwords expire in 180 day intervals.

Recommendation No. 4

We recommend MSU-Bozeman:

A. Restrict access to the audit journal file to the security officer and system

administrator.

B. Enable the security alarms INSTALL, LOGIN, and FILE_ACCESS.

Response No. 4

A. We concur. Access to the audit journal file will be limited to the security officer and the system administrator.

B. We concur. INSTALL, LOGIN failures, and FILE_ACCESS security alarms will be enabled.

Recommendation No. 5

We recommend MSU-Bozeman:

A. Restrict access to the critical application files to only those individuals needing it in the performance of their jobs.

B. Log and review all access to the critical application files.

Response No. 5

A. We concur. OSCS will implement this as an internal policy.

B. We concur. As part of the policy mentioned in (A) critical application files will be identified and access to them logged.

Recommendation No. 6

We recommend MSU-Bozeman:

A. Limit programmer access to production programs and data.

B. Log and review all programmer activity relating to the production programs and data.

Response No. 6

A. We concur. MSU-Bozeman understands the potential problems associated with direct programmer access to production programs and data. OSCS will strive to reach an ideal situation where there is no access, but the systems currently in production often require direct programmer intervention at this time.

B. We concur. Logging and review will commence immediately.

Recommendation No. 7

We recommend MSU-Bozeman:

A. Review the "verification" function, and enable it if security will be enhanced.

B. Disable the INCOMING parameter for the main cluster.

C. Review all proxy logins and eliminate unnecessary proxy logins with privileges.

Response No. 7

A. We concur. This function is being reviewed at this time.

B. We concur. We are in the process of reviewing all proxy accounts on the cluster to insure that disabling the INCOMING parameter will not cause problems with existing job streams. The review/stream modification will be complete by 1 July 1995.

C. We concur. OSCS is in the process of performing a review of all proxy accounts and writing an internal policy to insure an appropriate authorization and review process.

Recommendation No. 8

We recommend MSU-Bozeman require authorized access request forms for all individuals requesting privileges above the minimum.

Response No. 8

We concur. This has been completed as part of Response No. 1.

Recommendation No. 9

We recommend MSU-Bozeman:

A. Establish a detailed disaster recovery plan.

B. Test the plan.

Response No. 9

A. We concur. MSU-Bozeman's Operations Manager has attended a Disaster Recovery Seminar and is in the process of writing a comprehensive disaster recovery plan for the Montana State University System.

B. We concur. This will also be a part of the plan, to test on a regular basis.

Recommendation No. 10

We recommend MSU-Bozeman:

A. Schedule preventive maintenance and testing of existing environmental controls, and maintain documentation of the maintenance and testing completed.

B. Train OSCS employees on the proper use and maintenance of the environmental controls.

C. Ensure its off-site storage facility is located in a secure location where the risk of damage from environmental hazards is minimized.

Response No. 10

A. We concur. OSCS has contracted maintenance on some environmental controls, such as the halon system. Other devices such as water level alarms have been maintained on an ad hoc basis. This will become a formal process established via an internal policy.

B. We concur. This will be a part of the policy mentioned in (A).

C. We concur. The off-site storage has been moved.

Recommendation No. 11

We recommend MSU-Bozeman:

A. Restrict computer room access for systems programmers and custodians to hours when the room is staffed.

B. Enable the access logging function offered by the security contractor.

Response No. 11

A. We concur partially. OSCS Network Systems personnel require access to the machine room during off-hours.

B. We concur. This has been accomplished.

Recommendation No. 12

We recommend MSU-Bozeman:

A. Document Module Team review and approval of system changes.

B. Require authorized change request forms for system programming changes.

Response No. 12

A. We concur. This will be implemented in the form of an internal policy.

B We concur. This will be a part of the policy mentioned in (A).

Recommendation No. 13

We recommend MSU-Bozeman review present policies and procedures, and ensure critical processes are thoroughly documented, to ensure continuity of operations.

Response No. 13

We concur. There are two areas of computing policy and procedures on the MSU-Bozeman campus. Campus-wide issues are addressed via the University Computing Policy Committee (UCPC). This group has been established for many years, and they review campus computing on a yearly basis.

Internal OSCS computing policies and procedures need some work. We are reviewing and consolidating the policies and procedures that exist, and are aggressively correcting deficiencies in the areas of concern noted in this audit.